

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS


**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

**Conditional access system and smartcard allowing such access**

Patent Number: ☐ EP0817485  
Publication date: 1998-01-07  
Inventor(s): CAMPINOS ARNALDO (FR); FISCHER JEAN-BERNARD (FR)  
Applicant(s): THOMSON MULTIMEDIA SA (FR)  
Requested Patent: ☐ JP10164052  
Application Number: EP19970401382 19970617  
Priority Number(s): FR19960008053 19960628  
IPC Classification: H04N7/16 ; H04N7/167  
EC Classification: H04N7/16E2, H04N7/167D  
Equivalents: CN1171015, ☐ FR2750554, ☐ US6035038

**Abstract**

The invention relates to a conditional access system allowing a service provider to supply services only to those users who have acquired entitlements to these services. The services supplied by a service provider consist of an item scrambled by control words. In order to keep the control words secret, they are supplied after having been encrypted with an algorithm with key K. The entitlements of each user are forwarded in messages commonly denoted EMM (the abbreviation EMM standing for "Entitlement Management Messages"). According to the invention, the key K of the control words encryption algorithm is contained in the EMMs. 

Data supplied from the esp@cenet database - I2'

**Conditional access system and smartcard allowing such access**

Patent Number:      ☐ EP0817485  
Publication date:    1998-01-07  
Inventor(s):        CAMPINOS ARNALDO (FR); FISCHER JEAN-BERNARD (FR)  
Applicant(s)::      THOMSON MULTIMEDIA SA (FR)  
Requested Patent:   ☐ JP10164052  
Application Number: EP19970401382 19970617  
Priority Number(s): FR19960008053 19960628  
IPC Classification:   H04N7/16 ; H04N7/167  
EC Classification:    H04N7/16E2, H04N7/167D  
Equivalents:        CN1171015, ☐ FR2750554, ☐ US6035038

---

**Abstract**

---

The invention relates to a conditional access system allowing a service provider to supply services only to those users who have acquired entitlements to these services. The services supplied by a service provider consist of an item scrambled by control words. In order to keep the control words secret, they are supplied after having been encrypted with an algorithm with key K. The entitlements of each user are forwarded in messages commonly denoted EMM (the abbreviation EMM standing for "Entitlement Management Messages"). According to the invention, the key K of the control words encryption algorithm is contained in

the EMMs. 

---

Data supplied from the esp@cenet database - I2

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-164052

(43)公開日 平成10年(1998)6月19日

(51) Int.Cl.<sup>8</sup>

**識別記号**

FI

H04L 9/32

H04L 9/00

**6 7 3 C**

H04N 7/167

6 7 3 A

**6 7 3 B**

H04N 7/167

**z**

審査請求 未請求 請求項の数12 OL (全 7 頁)

(21)出願番号 特願平9-170262

(22)出願日 平成9年(1997)6月26日

(31)優先權主張番号 9608053

(32)優先日 1996年6月28日

(33)優先権主張国 フランス (FR)

(71)出願人 391000771

トムソン マルチメディア ソシエテ ア  
ノニム

THOMSON MULTIMEDIA  
S. A.

フランス国, 92648 プローニュ セデッ  
クス, ケ・アルフォンス・ル・ガロ 46

(72)発明者 アルナルド カンピノ

フランス国, 35000 レンヌ, ブルヴァ  
ル・ド・ラ・リベルテ 28

(72)発明者 ジャンーベルナール フィシエル

フランス国, 35700 レンヌ, リュ・ド・  
ヴァンセンヌ 9 a

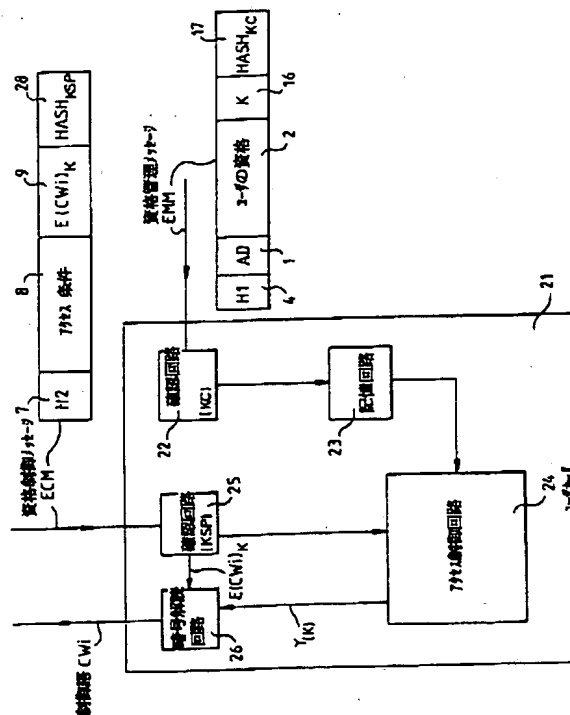
(74)代理人 弁理士 伊東 忠彦 (外1名)

(54) 【発明の名称】 条件付きアクセスシステム及び条件付きアクセスを許可するスマートカード

(57) 【要約】

【課題】 本発明は、サービスプロバイダがサービスに関する資格を得たユーザだけにサービスを提供し得る条件付きアクセスシステムを提案する。

【解決手段】 サービスプロバイダによって提供されるサービスは、制御語によりスクランブル処理された項目により構成される。制御語を秘密状態に保つため、制御語は、鍵Kを用いるアルゴリズムで暗号化された後に供給される。各ユーザの資格は、資格管理メッセージEMMで転送される。本発明によれば、制御語暗号化アルゴリズムの鍵Kは、メッセージEMMに含まれる。



【特許請求の範囲】

【請求項1】 鍵Kを用いるアルゴリズムで暗号化され

クランブル処理されユーザに提供されたサービスのスク  
ランブルを解除し得るスマートカードであって、

ランブル処理された項目により構成される。スクランブルされた項目は、資格が許可されたレベルのユーザしかスクランブル解除できないので、資格が許可されたレベルのユーザだけにより読まれる。以下では、ECG

(「電子的符号化品(Electronically Coded Good)」の略語)がスクランブル処理されていない項目を表わすとき、スクランブル処理された項目をIE(ECG)のように表わす。

【0003】スクランブル処理された項目のスクランブルを解除するため、サービスプロバイダは、項目をスクランブルするため用いられた制御語を各ユーザに配布する。制御語を秘密状態に保つため、制御語は、鍵Kを用いるアルゴリズムで暗号化された後に供給される。種々の暗号化された制御語は、一般的にECM(「資格制御メッセージ(Entitlement Control Message)」の略語)と称されるメッセージ中でユーザに転送される。

【0004】サービスプロバイダは、許可されたユーザだけに自分のサービスへのアクセス権を与えるため、許可された各ユーザにスマートカード及びデコーダを給付する。スマートカードは、一方で、ユーザが配布されたサービスに対し保有する資格を確認し、かつ、記録することが可能であり、他方で、暗号化された制御語を鍵Kを用いて解読できるようにする。この目的のため、スマートカードは、制御語の暗号化を行ったアルゴリズムの鍵Kを含む。デコーダは、スマートカードから送出される解読された制御語を含む項目に基づいて、スクランブル処理された項目のスクランブルを解除することが可能である。

【0005】各ユーザの資格は、一般的にEMM(「資格管理メッセージ(Entitlement Management Messages)」の略語)と称されるメッセージで転送される。従来技術によれば、ユーザ専用のEMMは、第1、第2及び第3の3個の主要項目により構成される。

—第1の項目はユーザのカードのアドレスを与える。

—第2の項目はユーザの資格の記述を与える。

—第3の項目は、EMMを確認し、かつ、EMMに含まれたユーザの資格が本当にそのユーザのため確保された資格であるかどうかを照合できるようにする。

【0006】ユーザのデコーダがサービスプロバイダにより与えられた種々のアドレスの中から自分に関係したカードのアドレスを認識するとき、認識されたアドレスに対応するEMMが解析される。EMMの解析は制御語を暗号化するための鍵Kに依存した解析アルゴリズムを用いて行われる。

【0007】

【発明が解決しようとする課題】制御語を暗号化するためのアルゴリズムの鍵Kは各ユーザカードに収容されている。従って、1枚のカードに対する侵害行為によって、鍵Kが突き止められる。サービスプロバイダによって供給され、同一の鍵Kを含む他の全てのカード上に、

不正なユーザ資格が作成され、記録される。侵害されたカードに含まれるユーザ資格を上記の他のカードに複製することも可能である。従って、プロバイダによって提供されるサービスは保護されなくなる。

【0008】上記の欠点を解決するため、制御語を暗号化するアルゴリズムの鍵を規則的な時間間隔で変更する方法がサービスプロバイダに知られている。この方法の場合、サービスプロバイダは新しい鍵Kを収納した新しいカードを各ユーザに供給しなければならない。ユーザカードの枚数は大抵非常に多いので、この方法は、特にコスト面で問題がある。ユーザカードの枚数は、実質的に数十万枚、或いは、数百万枚に達する場合が多い。

【0009】本発明は上記従来技術の欠点の解決を目的とする。

【0010】

【課題を解決するための手段】本発明は新規の条件付きアクセスシステムに係り、特に、新規の資格管理メッセージ(EMM)の定義、並びに、ユーザカードに収納される種々の機能の新規の定義に関する。従って、本発明によるメッセージは、鍵Kを伴うアルゴリズムによって暗号化された後にユーザに供給される制御語を用いてスクランブル処理された項目により構成されたサービスに対しユーザが保有する資格を定義するメッセージ(EMM)であって、上記メッセージは、該メッセージを確認し、かつ、該メッセージに含まれる資格が上記ユーザのため確保された資格であるかどうかを照合することができる項目を含む。上記メッセージ(EMM)は、制御語を暗号化するアルゴリズムの鍵Kを含む。

【0011】更に、制御語を用いてスクランブル処理され、少なくとも一人のユーザに提供されたサービスのスクランブルを解除する本発明の方法は、鍵Kを用いるアルゴリズムで暗号化された少なくとも1個の制御語を含む第1のメッセージ(ECM)を上記ユーザに供給する段階と、上記ユーザの資格を収容する第2のメッセージ(EMM)を上記ユーザに供給する段階と、上記第2のメッセージ(EMM)に収容された上記資格が上記ユーザのため確保された資格であるかを確認、照合する段階とからなる。鍵Kは上記第2のメッセージ(EMM)中に上記ユーザに与えられる。

【0012】鍵Kを用いるアルゴリズムで暗号化され、受信された制御語を暗号解読し、暗号解読後に、スクランブル処理されたサービスのスクランブルを解除する本発明のスマートカードは、ユーザの資格の確認を制御する第1の制御鍵を保有し、ユーザの資格を確認する回路と、第2の制御鍵を保有し、上記サービスと関係したアクセス条件を確認する回路とにより構成される。上記第1の制御鍵は上記鍵Kとは異なる。本発明の好ましい一実施例によれば、上記第1の制御鍵は上記カードに対し個別の鍵であり、従って、カード相互間で異なる。

【0013】更に、サービスプロバイダがサービスに対

する資格を得たユーザだけに制御語によってスクランブル処理された項目により構成されたサービスを提供することが可能になる本発明の条件付きアクセスシステムは、各ユーザに対する少なくとも1台のデコードと少なくとも1台のユーザカードとからなり、上記ユーザカードは、一方で、上記サービスプロバイダにより供給された上記サービスに対し、第1のメッセージ(EMM)により上記ユーザに伝達された上記ユーザの資格を確認、記録することが可能な回路と、他方で、鍵Kを伴うアルゴリズムにより暗号化され、第2のメッセージ(ECM)により上記ユーザカードに伝達された制御語から上記制御語を得ることが可能な回路とからなる。

【0014】上記ユーザカードは、上記の本発明によるスマートカードのようなカードであり、上記第1のメッセージ(EMM)は、上記本発明のメッセージのようなユーザによって保有される資格を定義し得るメッセージである。本発明によれば、プロバイダにより供給されたサービスの保護が非常に高められることである。1枚以上のユーザカードに対する侵害行為は、實際上、所謂権利侵害者に全く利益を与えない。

【0015】

【発明の実施の形態】以下、添付図面を参照して、本発明の好ましい実施例の説明を読むことにより、本発明の他の特徴及び利点が明らかになる。全図面を通して同一のラベルは同一の要素を表わす。図1の(a)には従来技術による第1の資格管理メッセージEMMフォーマットが示される。同図に示された資格管理メッセージEMMは、主要な3項目を含む本文C1aと、ヘッダ4とからなり、ヘッダの内容H1は、特に、本文C1aに含まれる項目のタイプ及びサイズを与える。

【0016】本文C1aは、ユーザのカードのアドレスADを格納する第1の項目1と、ユーザの資格の記述を格納する第2の項目2と、キューHASH<sub>K</sub>を格納する第3の項目3とにより構成される。キューHASH<sub>K</sub>は、鍵Kに依存して上記の資格管理メッセージEMMの解析が行えるようにする。図1の(b)は従来技術の第2の資格管理メッセージEMMフォーマットを示す。資格管理メッセージは、ヘッダ4と本文C1bとにより構成される。

【0017】本文C1bに含まれる項目5及び項目6は、夫々、ユーザのカードのアドレスAD、及び、鍵Kを用いたアルゴリズムで暗号化され、アドレスADと関係したユーザの資格の記述E(ユーザの資格)<sub>K, AD</sub>を含む。この資格管理メッセージEMMフォーマットによれば、資格管理メッセージEMMに含まれる資格の確認及び照合は、暗号化された資格の暗号解読の動作により行われる。

【0018】図2には従来技術による資格制御メッセージECMのフォーマットが示される。資格管理メッセージECMは本文C2及びヘッダ7により構成され、ヘッ

ダ7の内容H2は、特に、本文C2に含まれる項目のタイプ及びサイズを与える。本文C2は、特に、サービスプロバイダにより提供されたサービスと関係したアクセス条件の集合を格納する第1の項目8と、制御語Cwiを鍵Kを伴うアルゴリズムで暗号化した制御語E(Cwi)<sub>K</sub>を格納する第2の項目9と、鍵Kに依存し、アクセス条件の内容を確認及び照合し得るようにするキューHASH<sub>K</sub>を格納する第3の項目10とからなる。制御語Cwiは現時点の制御語、即ち、現時に読まれたプログラムの一部のスクランブルを解除させ得る制御語を表わす。

【0019】当業者に公知の如く、一般的に制御語Cwiを含む資格制御メッセージECMは第2の制御語を含む。第2の制御語は、次のスクランブル解除期間の制御語、即ち、現時の制御語としてCwiを格納する資格制御メッセージECMに追従すべき資格制御メッセージECMの現時の制御語である。この第2の制御語は、図面を無駄に複雑化させないように図2に示されていない。

【0020】当業者には公知の如く、資格制御メッセージEMMはサービスプロバイダによってスクランブル処理された項目IE(ECG)と共に転送される。図2に示された資格制御メッセージECMフォーマットは、資格制御メッセージECMフォーマットの一例に過ぎない。特に、図2に記載された資格制御メッセージECMを構築する種々のブロック(7, 8, 9, 10)の順番は、変更してもよい。

【0021】図3は従来技術のユーザカードの概要図である。ユーザカード11は、5個の主要な回路、即ち、ユーザの資格を確認する回路12と、確認されたユーザの資格を記憶する回路13と、アクセスを制御する回路14と、資格制御メッセージECMを確認する回路15と、暗号化された制御語を暗号解読する回路27とにより構成される。

【0022】資格管理メッセージEMMのフォーマット(例えば、図1の(a)及び(b)を参照のこと)とは無関係に、確認回路12は、資格管理メッセージEMMに基づいて上記のユーザアドレス認識及びユーザの資格の解析の動作を行う。この目的のため、確認回路12は暗号化アルゴリズムの鍵Kを保有する。資格管理メッセージEMMが確認されたならば、資格管理メッセージEMMに含まれたユーザの資格は確認された資格を記憶する回路13に格納される。

【0023】資格制御メッセージECMを確認する回路15は、ユーザの資格に基づいて確認回路12により行われた動作と同じ動作を、資格制御メッセージECMに含まれたアクセス条件8に基づいて行える。確認回路15は鍵Kを保有する。暗号解読回路27は制御語を暗号解読することが可能である。この目的のため、暗号解読回路27は制御語を暗号化するアルゴリズムの鍵Kを更に有する。

【0024】アクセス制御回路14は、確認されたアクセス条件を確認されたユーザの資格と比較する。確認されたアクセス条件が確認されたユーザの資格と対応するならば、アクセス制御回路14から送出され、暗号解読回路27に供給された信号Sは、確認回路15から発生した暗号化された制御語 $E(Cwi)_k$ の暗号解読を認証する。確認されたアクセス条件が確認されたユーザの資格と対応しない場合には、信号Sは暗号解読を認証しない。

【0025】暗号解読処理の種々の段階の終了時に、暗号解読された制御語 $Cwi$ は、スクランブル処理された項目IE(EG)のスクランブルが解除されるように暗号解読回路27により発生される。上記の如く、単一のユーザカードに対する侵害行為は、鍵Kへのアクセス権を許可し、プロバイダにより供給されたサービスの集合の保護を破壊する。

【0026】図4の(a)には本発明による第1の資格管理メッセージEMMフォーマットが示される。ユーザの資格管理メッセージEMMの本文C3aは、以下の4個の主要項目、即ち、ユーザのアドレス及びユーザの資格の記述を夫々構成する項目1及び2と、制御語を暗号化するアルゴリズムの鍵Kを収容する項目16と、KCが鍵Kとは異なる鍵を表わすとき、ハッシュキュー $HA SH_{KC}$ を収容する項目17とにより構成される。

【0027】本発明の好ましい実施例によれば、鍵KCは各ユーザ毎に固有であり、カード相互間で異なる。他の実施例によれば、鍵KCはユーザカードのグループ毎に固有である。図4の(b)には本発明による第2の資格管理メッセージEMMフォーマットが示される。同図を参照するに、資格管理メッセージEMMの本文C3bは、項目18、19及び20の主要3項目からなる。

【0028】項目18及び19は、ユーザカードのアドレスADと、鍵KCを備え、かつ、アドレスADに関係したアルゴリズムで暗号化されたユーザの資格の記述 $E(\text{ユーザの資格})_{KC, AD}$ とからなる。鍵KCは鍵Kとは異なる。本発明の好ましい実施例によれば、鍵KCは各ユーザカード毎に個別であり、カード相互間で相違する。他の実施例によれば、鍵KCはユーザカードのグループ毎に固有である。

【0029】上記資格管理メッセージEMMフォーマットによれば、資格管理メッセージEMMに収容された資格の確認及び照合は、暗号化された資格を暗号解読する動作により行われる。項目20は鍵KCによるアルゴリズムを用いて暗号化された制御語 $E(K)_{KC}$ を暗号化する鍵Kを含む。

【0030】資格管理メッセージEMMのフォーマットとは無関係に、資格管理メッセージEMMがユーザに伝送されない限り、制御語を暗号化する鍵Kがユーザのカードに保有されない点が有利である。図5は、本発明によるユーザカード、並びに、本発明による資格制御メッセ

ージECM及び資格管理メッセージEMMの概要図である。ユーザカード21は以下の5個の主要回路、即ち、ユーザの資格を確認する回路22と、ユーザの確認された資格を記憶する回路23と、アクセスを制御する回路24と、資格制御メッセージECMを確認する回路25と、暗号化された制御語を暗号解読する回路26とにより構成される。

【0031】図5の資格管理メッセージEMMは、図4の(a)に示されたタイプのメッセージである。本発明によるユーザカードは、図4の(b)に示された資格管理メッセージEMMとともに動作させてもよい。本発明によれば、資格管理メッセージEMMは、鍵KCで制御された確認アルゴリズムを用いて解析される。鍵KCは確認回路22に含まれる。

【0032】一方、資格制御メッセージECMは、鍵KSPで制御された確認アルゴリズムを用いて解析される。この目的のため、本発明の枠組みの範囲内で、資格制御メッセージECMは、鍵KSPに依存してキュー $HA SH_{KSP}$ を収容する項目28を含む。鍵KSPは確認回路25に保有される。鍵KSPは鍵Kとは異なる。本発明の好ましい実施例によれば、鍵KSPはサービスプロバイダ毎に固有である。

【0033】アクセス制御回路24は、確認されたアクセス条件を確認されたユーザの資格と比較する。確認されたアクセス条件が確認されたユーザの資格と対応するならば、アクセス制御回路24から送出され、暗号解読回路26に供給された信号Y(K)は、制御語の暗号解読を認証する。信号Y(K)は、鍵Kを暗号解読回路26に伝送するため鍵Kを保有する。暗号化された制御語 $E(Cwi)_k$ は、確認回路25から暗号解読26に転送される。次に、制御語の暗号解読が行われる。暗号解読処理の種々の段階の終了時に、暗号解読された制御語 $Cwi$ は、スクランブル処理された項目のスクランブルが解除され得るように、暗号解読回路26により発生される。

【0034】確認されたアクセス条件が確認されたユーザの資格に対応しない場合に、制御語の暗号解読は認証されない。本発明によれば、ユーザの資格の確認は、ユーザ又はユーザのグループ毎に個別の鍵KCによって制御される。従って、ユーザカードに対する侵害行為は、侵害行為を受けたカード自体だけを危険に晒し、並びに、鍵KCが全く同一のユーザのグループにより共有されている場合にそのユーザと同一グループ内のユーザカードだけを危険に晒す。従って、他の全てのユーザは保護され続ける点が有利である。

【0035】上記の本発明の実施例によれば、鍵Kはプロバイダにより供給された全てのサービスに対し同一である。本発明は、プロバイダにより供給された種々のサービスが、暗号化鍵がサービス相互間で相違し、或いは、サービスのグループ相互間で相違するアルゴリズム



により暗号化された制御語でスクランブル処理される実施例を実現する。

【0036】これによる利点は、特に、一般的に「オフライン」システムと称され、スクランブル処理された項目IE (ECG) 及び資格制御メッセージECMが、例えば、コンパクトディスク、デジタルビデオディスク、又は、他のCD-ROM (コンパクトディスク読み出し専用メモリ) のような自立型データ媒体に格納されているシステムの場合に得られる。

【0037】更に、ユーザカードに対する侵害行為は、プロバイダの全てのサービスが同一の鍵Kで暗号化された制御語を用いてスクランブル処理される場合よりも利益が欠ける点で有利である。従って、ユーザカードに対する侵害行為は、プロバイダによって提供される種々のサービスに関して非常に部分的なアクセスしか与えない。

【0038】例えば、映画のような種々のサービスをサービス相互間で鍵が相違するアルゴリズムを用いてスクランブル処理することは、サービスの制御語を暗号化するアルゴリズムの鍵と、ユーザの資格を確認するアルゴリズムに関連した鍵とが同一である従来技術の条件付きアクセスシステムの枠組みの範囲内では考えられなかった。従って、サービスプロバイダは、各サービス又はサービスのグループ毎に個別のカードを各ユーザに供給する必要があった。このようなカードの数の増加は、実用上の理由及び費用的な理由の両面で非現実的である。

【0039】一般的に言うと、本発明の実施例の形態に左右されることなく、即ち、プロバイダによって提供された種々のサービスが制御語を暗号化する単一の鍵Kに關係しているか、或いは、異なる暗号化鍵 $K_j$  ( $j = 1, 2, \dots, m$ ) に關係しているかには係わらず、

本発明は、「オフライン」タイプの条件付きアクセスシステムだけではなく、スクランブル処理された項目IE (ECG) が単一の信号源からサービスプロバイダの種々の顧客に同時に配布された信号により構成された項目である「オンライン」タイプの条件付きアクセスシステムにも適用される。

【0040】

【発明の効果】本発明によれば、プロバイダにより提供されたサービスの保護が非常に高められる利点が得られる。1枚以上のユーザカードに対する侵害行為は、實際上、所謂権利侵害者に対し、全く利益を与えない。

【図面の簡単な説明】

【図1】(a) 及び (b) は、夫々、従来技術による第1及び第2の資格管理メッセージ (EMM) のフォーマットを表わす図である。

【図2】従来技術による資格制御メッセージ (ECM) のフォーマットを表わす図である。

【図3】従来技術によるユーザカードの概要図である。

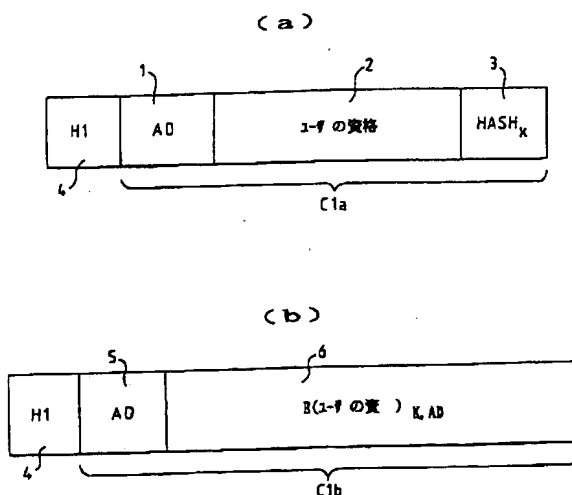
【図4】(a) 及び (b) は、夫々、本発明による第1の資格管理メッセージ (EMM) フォーマット及び第2の資格管理メッセージ (EMM) フォーマットを表わす図である。

【図5】本発明によるユーザカードの概要図である。

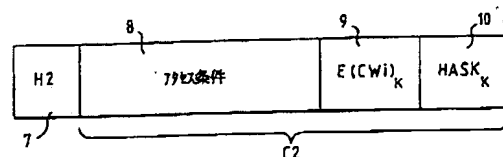
【符号の説明】

- 11, 21 ユーザカード
- 12, 22 ユーザ資格確認回路
- 13, 23 ユーザ資格記憶回路
- 14, 24 アクセス制御回路
- 15, 25 資格制御メッセージ確認回路
- 26, 27 暗号解読回路

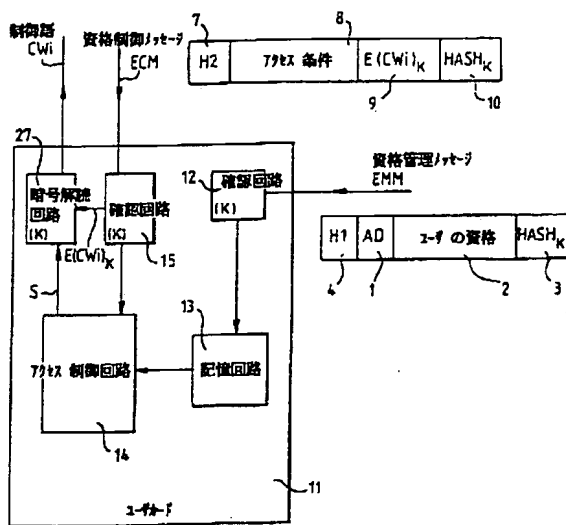
【図1】



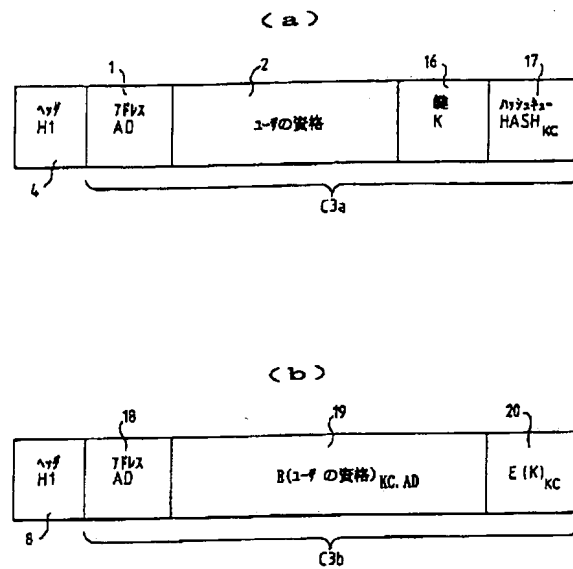
【図2】



【図3】



【図4】



【図5】

